NUMBER FIELDS WITHOUT SMALL GENERATORS

JEFFREY D. VAALER AND MARTIN WIDMER

Abstract. Let $D > 1$ be an integer, and let $b = b(D) > 1$ be its smallest divisor. We show that there are infinitely many number fields of degree D whose primitive elements all have relatively large height in terms of b, D and the discriminant of the number field. This provides a negative answer to a questions of W. Ruppert from 1998 in the case when D is composite. Conditional on a very weak form of a folk conjecture about the distribution of number fields, we negatively answer Ruppert's question for all $D > 3$.

1. Introduction

Let $H(\cdot)$ be the absolute multiplicative Weil height on the algebraic numbers $\overline{\mathbb{Q}}$, as defined in, e.g., [2], and let $L \subset \overline{\mathbb{Q}}$ be a number field of degree $D > 1$. We are interested in bounds, expressed in terms of the degree D and the absolute discriminant Δ_L of L, for the smallest height of a generator. It is convenient to use the following invariant, introduced by Roy and Thunder [6],

$$\delta(L) = \inf\{H(\alpha); L = \mathbb{Q}(\alpha)\}.$$

By Northcott's Theorem the infimum is attained, and hence, $\delta(L)$ denotes the smallest height of a generator of the extension L over $\mathbb{Q}$. Silverman [9, Theorem 1] has shown that

$$\delta(L) \geq D^{-\frac{1}{2(D-1)}} |\Delta_L|^{\frac{1}{2D(D-1)}}. \tag{1.1}$$

The following example due to Ruppert [7, p.18] and Masser [6, Proposition 1]) shows that in this general situation the exponent $1/(2D(D-1))$ cannot be improved. Let p and q be primes that satisfy $0 < p < q < 2p$. Let $\alpha = (p/q)^{1/D}$, and let $L = \mathbb{Q}(\alpha)$. Then, by the Eisenstein criterion, L has degree D, and p and q are both totally ramified in L. Hence, $(pq)^{D-1}|\Delta_L$, and thus

$$H(\alpha) = q^{\frac{1}{D}} \leq (2pq)^{\frac{1}{2D}} \leq 2^{\frac{1}{2D}} |\Delta_L|^{\frac{1}{2D(D-1)}}. \tag{1.2}$$

Ruppert [7, Question 1] asked whether the exponent is always sharp, more precisely he proposed the following question.

Question 1.1 (Ruppert, 1998)**.** Is there a constant C_D such that for all number fields L of degree D

$$\delta(L) \leq C_D |\Delta_L|^{\frac{1}{2D(D-1)}}?$$

In fact Ruppert used the naive height but elementary inequalities between the naive and the Weil height show that Ruppert's question is equivalent to the one stated above. Ruppert [7, Proposition 2] himself answered this question in the affirmative for $D = 2$. The aim of this note is to answer Ruppert's question in the negative for all composite D.

Date: October 18, 2014, and in revised form ....
1991 *Mathematics Subject Classification.* Primary 11R04, 11G50; Secondary 11R06, 11R29.
Key words and phrases. Algebraic number theory, small height.

Theorem 1.2. *Let $b = b(D) > 1$ be the smallest divisor of D, and suppose γ is a real number such that*

$$\gamma < \begin{cases} 1/(D(b+1)) : & \text{if } b \leq 3, \\ 1/(2D(b+1)) + 1/(Db^2(b+1)) : & \text{otherwise.} \end{cases}$$

Then there exist infinitely many number fields L of degree D satisfying

$$\delta(L) > |\Delta_L|^\gamma.$$

Note that for composite $D > 4$ we have

$$\frac{1}{2D(b+1)} + \frac{1}{Db^2(b+1)} > \frac{1}{2D(\sqrt{D}+1)} > \frac{1}{2D(D-1)}.$$

Thus, Theorem 1.2 provides a negative answer to Question 1.1 for all composite D. In fact, we prove a stronger result, namely: let F be any number field of degree D/b; when enumerated by the modulus of the discriminant, the subset of all degree b extensions L of F, defined by $\delta(L) > |\Delta_L|^\gamma$, has density 1 (for the precise statement we refer to Corollary 4.1).

Our proof strategy requires a good lower bound for the number of degree D fields with bounded modulus of the discriminant. Essentially optimal bounds are available when D is even or divisible by 3, and if D is composite we still have some useful bounds. However, a folk conjecture (sometimes attributed to Linnik) predicts the asymptotics $c_D T$ as T goes to infinity, for some constant $c_D > 0$. Unfortunately, the best general lower bounds are only of order $T^{1/2+1/D^2}$ which is just slightly weaker than what we need. Therefore, our next result is conditional.

Theorem 1.3. *Suppose that $D > 3$, and suppose that there exist constants $c_D > 0$ and $\nu_D > 1/2 + 1/(D-1)$ such that the number of degree D fields $L \subset \overline{\mathbb{Q}}$ with absolute value of the discriminant no larger than T is at least $c_D T^{\nu_D}$ for all T large enough. Then there exists $\gamma > 1/(2D(D-1))$ such that there are infinitely many number fields L of degree D with*

$$\delta(L) > |\Delta_L|^\gamma.$$

Thanks to [1], the hypothesis of Theorem 1.3 is satisfied for $D = 5$, and hence we get an unconditional negative answer to Question 1.1 for $D = 5$. Furthermore, Theorem 1.3 shows that most likely the answer to Question 1.1 is "no" for all $D > 3$. However, our method sheds no light on the case $D = 3$.

In this article we use Vinogradov's notation $\ll$ and $\gg$ at various places. The involved constants are allowed to depend on all quantities except on the parameter T, which is introduced in the next section.

2. Enumerating fields: discriminant versus delta-invariant

Any number field is considered a subfield of the fixed algebraic closure $\overline{\mathbb{Q}}$. Let k be a number field, let $m = [k : \mathbb{Q}]$, let L/k be a finite extension of degree $d = [L : k] > 1$, and put $D = [L : \mathbb{Q}] = md$. For the remainder of this paper we set

$$\mathcal{C} = \mathcal{C}_d(k) = \{L \subset \overline{\mathbb{Q}}; [L : k] = d\}, \tag{2.1}$$

and for a subset $S \subset \mathcal{C}$, and $\gamma \geq 0$ we set

$$S_\gamma = \{L \in S; \delta(L) > |\Delta_L|^\gamma\}. \tag{2.2}$$

We want to enumerate the fields in S in two different ways: once by the discriminant (more precisely, the modulus thereof), and once by the delta invariant $\delta(\cdot)$. Thus we introduce the counting functions

$$N_\Delta(S,T) = |\{L \in S; |\Delta_L| \le T\}|,$$
$$N_\delta(S,T) = |\{L \in S; \delta(L) \le T\}|.$$

Note that both cardinalities are finite; the first one by Hermite's Theorem, the second one by Northcott's Theorem. Next we introduce the set of generators of fields of S

$$P_S = \{\alpha \in \overline{\mathbb{Q}}; \mathbb{Q}(\alpha) \in S\},$$

and its counting function

$$N_H(P_S,T) = |\{\alpha \in P_S; H(\alpha) \le T\}|.$$

Again, the above cardinality is finite by Northcott's Theorem.

The proof of Theorem 1.2 is based on two simple observations, the first of which, is presented as the following proposition.

Proposition 2.1. *Suppose there are positive reals η, θ, and $\gamma < \eta/\theta$ such that $N_\Delta(S,T) \gg T^\eta$ and $N_H(P_S,T) \ll T^\theta$ for all T large enough. Then*

$$\lim_{T\to\infty} \frac{N_\Delta(S_\gamma,T)}{N_\Delta(S,T)} = 1.$$

Proof. Directly from the definitions we get

$$N_\Delta(S\backslash S_\gamma,T) \le N_\delta(S\backslash S_\gamma,T^\gamma) \le N_\delta(S,T^\gamma).$$

The map $\alpha \to \mathbb{Q}(\alpha)$ yields a surjection from $\{\alpha \in P_S; H(\alpha) \le T^\gamma\}$ to $\{L \in S; \delta(L) \le T^\gamma\}$. Hence, we have

$$N_\delta(S,T^\gamma) \le N_H(P_S,T^\gamma).$$

On the other hand, by the hypothesis,

$$N_H(P_S,T^\gamma) \ll T^{\gamma\theta},$$

and

$$N_\Delta(S,T) \gg T^\eta,$$

provided T is large enough. We conclude

$$\lim_{T\to\infty} \frac{N_\Delta(S\backslash S_\gamma,T)}{N_\Delta(S,T)} = 0,$$

whenever $\gamma < \frac{\eta}{\theta}$ which proves the proposition. □

3. Bounds for the counting functions

In view of Proposition 2.1 we want to find a set $S \subset \mathcal{C}$ that maximizes the ratio η/θ. Taking $S = \mathcal{C}_b(F) \subset \mathcal{C}$ as the set of fields that contain a fixed extension F/k of degree d/b does not affect η in a negative way as we shall see in Lemma 3.1, but it positively affects θ as we shall see in Lemma 3.2. This is the second simple but important observation for the proof of Theorem 1.2.

We start with lower bounds for η, that is, lower bounds for $N_\Delta(\mathcal{C}_b(F),T)$.

Lemma 3.1. *Let $b = b(d) > 1$ be the smallest divisor of d, and let F be an extension of k of degree d/b. Then we have*

$$N_\Delta(\mathcal{C}_b(F),T) \gg T^{1/2+1/b^2} \tag{3.1}$$

for all T large enough. If d is even or divisible by 3 then we even have

$$N_\Delta(\mathcal{C}_b(F),T) \gg T, \tag{3.2}$$

for all T large enough.

Proof. First we recall that for $L \in \mathcal{C}_b(F)$ we have $|\Delta_L| = |\Delta_F|^b N_{F/\mathbb{Q}}(\mathfrak{D}_{L/F})$, where $N_{F/\mathbb{Q}}(\cdot)$ is the absolute norm, and $\mathfrak{D}_{L/F}$ is the relative discriminant. Thus, counting fields in $\mathcal{C}_b(F)$ with $|\Delta_L| \leq T$ is the same as counting fields in $\mathcal{C}_b(F)$ with $N_{F/\mathbb{Q}}(\mathfrak{D}_{L/F}) \leq T/|\Delta_F|^b$. Therefore, Ellenberg and Venkatesh's [5, Theorem 1.1] shows that

$$N_\Delta(\mathcal{C}_b(F), T) \geq c' T^{1/2+1/b^2}$$

for some $c' = c'(b, F) > 0$ and all T large enough. This yields (3.1). For (3.2) we note that the conjectured asymptotic formula

$$N_\Delta(\mathcal{C}_b(F), T) = cT + o(T),$$

where $c = c(b, F) > 0$, has been proven by Datskovsky and Wright for $b = 2$ [3, Theorem 4.2] (see also [4, Corollary 1.2]) and for $b = 3$ [3, Theorem 1.1]. This proves the lemma. □

Next we establish an upper bound for $N_H(P_{\mathcal{C}_b(F)}, T)$. Recall that k is a number field of degree m, and also recall the notation $\mathcal{C} = \mathcal{C}_d(k)$ from (2.1).

Lemma 3.2. *We have for all $T > 0$*

$$N_H(P_{\mathcal{C}}, T) \ll T^{md(d+1)}. \tag{3.3}$$

With the notation of Lemma 3.1, in particular,

$$N_H(P_{\mathcal{C}_b(F)}, T) \ll T^{md(b+1)}. \tag{3.4}$$

Proof. First we note that $\mathbb{Q}(\alpha) \in \mathcal{C} = \mathcal{C}_d(k)$ implies $[k(\alpha) : k] = d$. Therefore,

$$N_H(P_{\mathcal{C}}, T) \leq |\{\alpha \in \overline{\mathbb{Q}}; [k(\alpha) : k] = d, H(\alpha) \leq T\}|.$$

Now Schmidt [8, Theorem] has shown that

$$|\{\alpha \in \overline{\mathbb{Q}}; [k(\alpha) : k] = d, H(\alpha) \leq T\}| \leq C(m, d) T^{md(d+1)}.$$

Therefore $N_H(P_{\mathcal{C}}, T) \leq C(m, d) T^{md(d+1)}$, which proves (3.3). □

4. Density results

Recall the notation in (2.2).

Corollary 4.1. *Let $b = b(d) > 1$ be the smallest divisor of d, and suppose γ is a real number such that*

$$\gamma < \begin{cases} 1/(md(b+1)) : & \text{if } b \leq 3, \\ 1/(2md(b+1)) + 1/(mdb^2(b+1)) : & \text{otherwise.} \end{cases}$$

Let F be an extension of k of degree d/b and let $B = \{L \in \mathcal{C}; F \subset L\}$. Then

$$\lim_{T\to\infty} \frac{N_\Delta(B_\gamma, T)}{N_\Delta(B, T)} = 1.$$

Proof. First note that $B = \mathcal{C}_b(F)$. Thus (3.1) yields $N_\Delta(B, T) \gg T^{1/2+1/b^2}$ for T large enough. If d is even or divisible by 3 then by (3.2) we even have $N_\Delta(B, T) \gg T$ for T large enough. On the other hand (3.4) gives $N_H(P_B, T) \ll T^{md(b+1)}$. Applying Proposition 2.1 with $S = B$ yields the statement. □

So almost all fields in $B = \mathcal{C}_b(F)$ satisfy $\delta(L) > |\Delta|^\gamma$. Note that, of course, B is an infinite set, and so Theorem 1.2 follows from Corollary 4.1 by taking $k = \mathbb{Q}$.

Corollary 4.2. *Suppose $\gamma < 1/(md(d+1))$ and suppose d is even or divisible by 3 then*

$$\lim_{T\to\infty} \frac{N_\Delta(\mathcal{C}_\gamma, T)}{N_\Delta(\mathcal{C}, T)} = 1.$$

Proof. Let F be an extension of k of degree $d/2$ if d is even, and of degree $d/3$ otherwise. Hence, $\mathcal{C} \supset \mathcal{C}_2(F)$ or $\mathcal{C} \supset \mathcal{C}_3(F)$ respectively, and so we conclude from (3.2) that $N_\Delta(\mathcal{C}, T) \gg T$. Furthermore, by (3.3) we have $N_H(P_\mathcal{C}, T) \ll T^{md(d+1)}$. Applying Proposition 2.1 with $S = \mathcal{C}$ yields the statement. □

Finally, to prove Theorem 1.3 we apply Proposition 2.1 with $S = \mathcal{C}$, $k = \mathbb{Q}$, $\eta = \nu_D > 1/2 + 1/(D-1)$ and $\theta = D(D+1)$ (for the latter we have applied (3.3)). As $\eta/\theta > 1/(2D(D-1))$ we conclude that there exists $\gamma > 1/(2D(D-1))$ such that there exist infinitely many number fields L of degree D that satisfy

$$\delta(L) > |\Delta_L|^\gamma.$$

This proves Theorem 1.3.

5. Cluster points

We consider the set of values

$$\frac{\log \delta(L)}{\log |\Delta_L|}$$

as L runs over all number fields of fixed degree $D > 1$. What are the cluster points of this set? Combining (1.1) and (1.2) gives the smallest cluster point

$$\lim \inf_{[L:\mathbb{Q}]=D} \frac{\log \delta(L)}{\log |\Delta_L|} = \frac{1}{2D(D-1)}.$$

What about the largest cluster point? With $b = b(D)$ as in Theorem 1.2 the latter implies that

$$\lim \sup_{[L:\mathbb{Q}]=D} \frac{\log \delta(L)}{\log |\Delta_L|} \geq \begin{cases} 1/(D(b+1)) : & \text{if } b \leq 3, \\ 1/(2D(b+1)) + 1/(b^2(b+1)D) : & \text{otherwise.} \end{cases}$$

If D is odd [10, Theorem 1.2] or if the Dedekind zeta-function associated to the Galois closure of L satisfies the Generalized Riemann Hypothesis for all number fields L of degree D, then [10, Theorem 1.3]

$$\lim \sup_{[L:\mathbb{Q}]=D} \frac{\log \delta(L)}{\log |\Delta_L|} \leq 1/(2D).$$

However, the best known unconditional general upper bound for the largest cluster point is $1/D$, see, e.g., [11, Lemma 4.5]. It might be an interesting problem to study the distribution of the cluster points, and to locate new cluster points.

Acknowledgments

Parts of this article were discussed and written during the special semester "Heights in Diophantine Geometry, Group Theory and Additive Combinatorics" held at the Erwin Schrödinger International Institute for Mathematical Physics.

References

1. M. Bhargava, *The density of discriminants of quintic rings and fields*, Ann. of Math. **172** (2010), 1559–1591.
2. E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, Cambridge University Press, 2006.
3. B. Datskovsky and D. J. Wright, *Density of discriminants of cubic field extensions*, J. reine angew. Math. **386** (1988), 116–138.
4. H. Cohen F. Diaz Y Diaz and M. Olivier, *Enumerating quartic dihedral extensions of* $\mathbb{Q}$, Comp. Math. **133** (2002), 65–93.
5. J. Ellenberg and A. Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. **163** (2006), 723–741.
6. D. Roy and J. L. Thunder, *A note on Siegel's lemma over number fields*, Monatsh. Math. **120** (1995), 307–318.

7. W. Ruppert, *Small generators of number fields*, Manuscripta math. **96** (1998), 17–22.
8. W. M. Schmidt, *Northcott's Theorem on heights I. A general estimate*, Monatsh. Math. **115** (1993), 169–183.
9. J. Silverman, *Lower bounds for height functions*, Duke Math. J. **51** (1984), 395–403.
10. J. D. Vaaler and M. Widmer, *A note on small generators of number fields*, Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms, Contemporary Mathematics, vol. 587, Amer. Math. Soc., Providence, RI, 2013.
11. M. Widmer, *Counting points of fixed degree and bounded height*, Acta Arith. **140.2** (2009), 145–168.

Department of Mathematics, University of Texas at Austin, 1 University Station C1200, Austin, Texas 78712

E-mail address: `vaaler@math.utexas.edu`

Department of Mathematics, Royal Holloway, University of London, TW20 0EX Egham, UK

E-mail address: `martin.widmer@rhul.ac.uk`